PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 17/00 — A1

(11) International Publication Number: **WO 99/66422**

(43) International Publication Date: 23 December 1999 (23.12.99)

(21) International Application Number: PCT/US99/13488

(22) International Filing Date: 15 June 1999 (15.06.99)

(30) Priority Data:
60/089,212 15 June 1998 (15.06.98) US

(63) Related by Continuation (CON) or Continuation-in-Part (CIP) to Earlier Application
US 08/485,269 (CIP)
Filed on 7 June 1995 (07.06.95)

(71) Applicant *(for all designated States except US)*: ASCOM HASLER MAILING SYSTEMS, INC. [US/US]; 19 Forest Parkway, P.O. Box 858, Shelton, CT 06484-0904 (US).

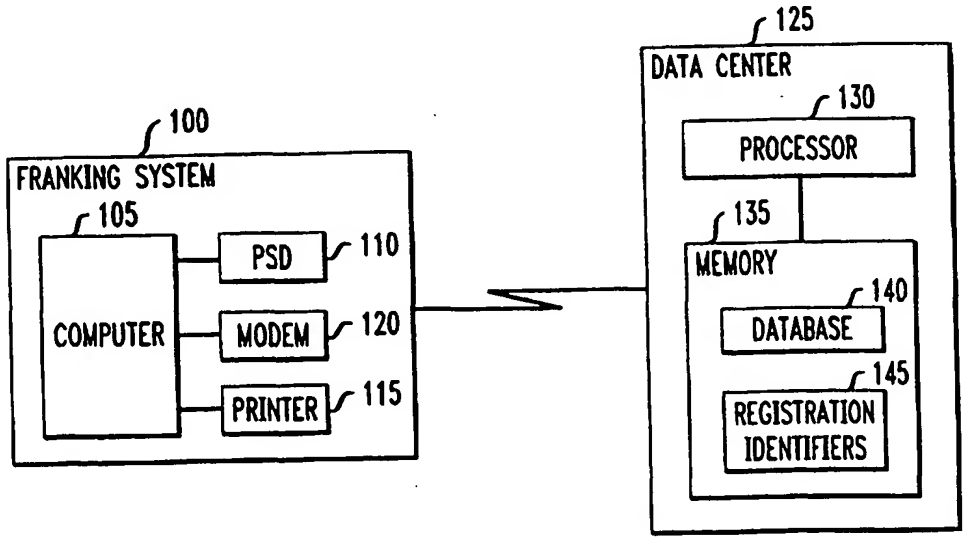
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: SCHWARTZ, Robert, G. [US/US]; 191 Linden Avenue, Branford, CT 06405 (US). BROOKNER, George, M. [US/US]; 11 Surrey Drive, Norwalk, CT 06851 (US). ESKANDARI, Fetneh [IR/US]; 144 Dove Lane, Middletown, CT 06457 (US). CROWE, Allen, A. [US/US]; 76 Klein Drive, Prospect, CT 06712 (US). SIMCIK, Mark, E. [US/US]; 141 Park Avenue, Bloomfield, CT 06002 (US).

(74) Agent: YIP, Alex, L.; Londa & Traub LLP, 37th floor, 20 Exchange Place, New York, NY 10005 (US).

(81) Designated States: CA, JP, US, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: TECHNIQUE FOR SECURING A SYSTEM CONFIGURATION OF A POSTAGE FRANKING SYSTEM



(57) Abstract

In a franking system a postal security device (PSD) tracks a postage fund for dispensing postal indicia and enforce the configuration of the franking system. An authorization code, which is particular to the system, is used to verify the system configuration. An unauthorized change in the system configuration causes invalidation of the code and generation of the postal indicia is denied. Data center (125) records configuration information of each franking system (100). The data center generates a valid authorization code for verification in the franking system based on new configuration information. Components added to the system must be preapproved to prevent fraudulent generation of postage indicia. A registration number is assigned to each preapproved component which is necessary for interaction with the franking system.

Description

TECHNIQUE FOR SECURING A SYSTEM CONFIGURATION OF A POSTAGE FRANKING SYSTEM

Technical Field

The invention relates to a secure system configuration technique, and more particularly to a technique for protecting the integrity of components in a postage franking system.

Background of the Invention

It is commonplace to use postage meters or franking systems for generating postage indicia on mailpieces. The format of the postage indicia is specified by a postal authority to facilitate its inspection. In the United States, much attention has been focused on an Information-Based Indicia Program (IBIP) by the United States Postal Service (USPS), proposing, among other things, new requirements for the format of a postage indicium. Such new requirements were promulgated, e.g., in the "Information Based Indicia Program (IBIP) Open System Indicium Specification," dated August 19, 1998. For instance, the IBIP requires inclusion of a 2-dimensional (2-D) barcode in the postage indicium. Such a barcode represents postal information including postage, and a digital signature for authenticating the postal information, in accordance with a public key algorithm. One such public key algorithm may be the Digital Signature Algorithm (DSA) described,

fraudulent manipulation to generate unauthorized postage indicia.

Summary Of the Invention

In accordance with the invention, an authorization code is used to secure the configuration of a franking system. The authorization code is derived in part from system configuration information concerning, e.g., the enabled and disabled feature options, current version number of software, and the identity of a computer in the franking system (e.g., the serial number of the computer). Any unauthorized change in the system configuration results in an invalidation of the authorization code in the franking system, and denial of the franking operation. Thus, any system reconfiguration, e.g., a change in the feature options or software upgrade, must be effected using a new valid authorization code. Preferably, the authorization code verification is performed each time before the franking operation starts to forestall any fraudulent generation of postage indicia.

In accordance with an aspect of the invention, software code, e.g., the object code of a postage generation program, in the franking system is subject to error checking thereof. Thus, the above authorization code is also derived from error checking information, e.g., cyclic redundancy check (CRC) bits or checksum of the software code. Any tampering of the software also results in an invalidation of the authorization code.

In addition, to minimize the risk of fraudulent generation of postage indicia, franking-related software and hardware components by, e.g., third party vendors,

through a communication connection with the data center. Such an online transaction involves the data center's downloading the software to, or enabling the feature option of, the franking system through the communication connection, with the price of the software or feature option debited from its customer account in the data center.

Brief Description of the Drawing

Further objects, features and advantages of the invention will become apparent from the following detailed description taken in conjunction with the accompanying figures showing illustrative embodiments of the invention, in which:

Fig. 1 illustrates a franking system which is capable of communicating with a remote data center in accordance with the invention;

Fig. 2 illustrates the format of each record in a database in the remote data center;

Fig. 3 is a block diagram of a postal security device used in the franking system;

Fig. 4 is a flow chart depicting the steps of a postage generation program used in the franking system;

Fig. 5 illustrates a postage indicium generated by the postage generation program;

Fig. 6 illustrates an authorization code which needs to be verified in reconfiguring the franking system;

Fig. 7 is a flow chart depicting the steps taken by the franking system to verify the authorization code;

serving as a host device, and where PSD 110, printer 115 and modem 120 are peripherals to computer 105. Alternatively, computer 105 may be a workstation or any other general purpose computing machine. Computer 105 may cause modem 120 to establish a communication connection through a communications network to, say, remote data center 125. Although modem 120 in this instance is shown as an external modem, it will be appreciated that any internal modem within computer 105 may be used, instead.

Data center 125 includes processor 130 which, among other things, maintains database 140 and registration identifiers 145 stored in memory 135 to serve different franking systems, e.g., franking system 100, communicates therewith to replenish their postage funds, and provides authorization codes to control their configurations in accordance with the invention.

Database 140 contains records concerning the respective franking systems served by data center 125. Fig. 2 illustrates the format of each record in database 140. In this instance, each franking system is identified by a PSD serial number in field 161 pre-assigned to its PSD. Field 163 contains account information such as a prefunded or credit escrow account balance for the franking system for conducting a telemeter setting (TMS) transaction described below. Field 165 includes configuration information (described below) concerning the configuration of the franking system to protect its integrity in accordance with the invention.

Fig. 3 illustrates PSD 110 which in this instance is realized as an integrated circuit (IC) module peripheral to computer 105. PSD 110 comprises secure

well known manner the current ascending and descending register values and other PSD data in secure memory 200 of PSD 110, and ascertains the availability of funds in the prefunded or credit escrow account of system 100. After the PSD data is validated and the account balance is found to be sufficient, processor 130 debits the account and remotely resets descending register 235 in PSD 110 accordingly.

System 100 in this instance may be used to generate postage indicia in accordance with the United States Postal Service (USPS) Information Based Indicia Program (IBIP) specification, namely, the "Information Based Indicia Program (IBIP) Open System Indicium Specification," dated August 19, 1998. To that end, secure memory 200 also includes a well-known digital signature algorithm (DSA) described, e.g., in "Digital Signature Standard (DSS)," FIPS PUB 186, May 19, 1994; and a private key and the corresponding public key in accordance with the DSA. The public key may be made available to the public in a PSD certificate in the postage indicia. For instance, using the DSA, unit 210 may sign specified postal data with an associated private key to generate a different digital signature to be included in each postage indicium. The postal authority then scans the postage indicium and verifies the digital signature to authenticate the postage indicium, in accordance with the DSA. It should be noted that instead of the DSA of the DSS, another well-known data authentication algorithm such as the RSA or Elliptic Curve algorithm may be used.

For postage franking operation, computer 105 is loaded with software components including postage generation program 300 for generating postage indicia.

indicium and pass it onto computer 105. Upon receiving a print command, computer 105 transmits the print image to printer 115, which then prints the postage indicium on a label or an envelope fed to printer 115.

Fig. 5 illustrates one such postage indicium 500 which serves as proof of postage payment. Indicium 500 includes human readable portion 555 and machine readable portion 560. Portion 555 may include, e.g., the date of mailing, postage, device ID, originating town and zip code, mail class, etc. Machine readable portion 560, which is readable using an optical scanner, may include a 2-dimensional barcode representing data concerning the device ID, ascending and descending register values, postage value, digital signature, date of mailing, licensing zip code, software ID, PSD certificate, mail class, etc. Alternatively, machine readable portion 560 may comprise one or more data matrix symbols representing similar data, as described in PCT International Publication No. WO 99/16023, published on April 1, 1999.

Because of the open system configuration of franking system 100, the user has full access to hardware and software components in system 100. As a result, these components, e.g., postage generation program 300 described above, are subject to tampering and unauthorized use. In accordance with the invention, verification of an authorization code is required from time to time to prevent tampering and unauthorized use of the components of system 100.

Fig. 6 illustrates one such authorization code 600 used to prevent any tampering and unauthorized use of postage generation program 300 described above, and feature options available in system 100 which may include, e.g., a label printing option and other printer

provided in field 165 of the record pertaining to system 100 in database 140.

It should be noted at this point that item (e) in this instance is obtained by running a well known CRC algorithm, e.g., Reed Solomon CRC algorithm, on the object code of program 300 which is authorized in system 100. Alternatively, a checksum derived in a conventional manner from the object code may be used.

The derivation by processor 130 of electronic signature 605 involves encrypting the combination of items (a) through (f) in accordance with a first well known encryption algorithm. Signature 605 is then derived from the encrypted version of the combination of the items, e.g., by extracting therefrom a predetermined sequence of m bits. Alternatively, signature 605 may be generated using a well known symmetric or asymmetric key cryptographic methodology.

On the other hand, encrypted option segment 610 is generated by encrypting only the option number (f) in accordance with a second well known encryption algorithm. Alternatively, segment 610 may be unencrypted, i.e., containing the plain text of option number (f).

It suffices to know for now that after system 100 enters a reconfiguration mode where authorization code 600 is entered, code 600 is stored in authorization code buffer 241. Encrypted option segment 610 of code 600 is subsequently decrypted to recover the underlying option number. Using the recovered option number (f) and additional items in system 100 which are identical to aforementioned items (a) through (e), and the same first encryption algorithm in the above-described manner, system 100 is capable of independently generating an electronic signature identical to electronic signature

code needs to be entered on system 100 while in a reconfiguration mode, causing the bit in the option number (f) corresponding to the label printing option to change to the opposite value to enable the option. System 100 effects the feature options according to the bit pattern of the option number stored in option number buffer 243 in memory 200. In this particular illustrative embodiment, the recovered option number from decrypting segment 610 of authorization code 600 overwrites the current option number in buffer 243 irrespective of the outcome of the validation of authorization number 600. That is, system 100 immediately effects the feature options according to the recovered option number as soon as it is placed in buffer 243, irrespective of the outcome of the validation.

After the feature options are effected in the prescribed manner in the reconfiguration mode, system 100 returns to a normal operation mode. When postage generation program 300 is invoked to perform the franking operation in the normal operation mode, unit 210 reads from memory 200 (i) the serial number of computer 105, (ii) the hardware configuration identifier of computer 105, (iii) the serial number of PSD 110, and (iv) the software version number of program 300, which are collected by unit 210 and stored in memory 200. Unit 210 also obtains (v) CRC bits based on running the aforementioned CRC algorithm on the latest code of program 300 in system 100, and (vi) the option number from buffer 243. Unit 210 independently generates an electronic signature using items (i) through (vi) and the aforementioned first encryption algorithm in a similar manner to processor 130 generating electronic signature 605 in data center 125. The electronic signature, thus

After the software installation or upgrade in the reconfiguration mode, system 100 returns to the normal operation mode. When postage generation program 300 is invoked to perform the franking operation in the normal operation mode, the user is prompted for authorization code 600 on the storage medium package. Authorization code 600 is then verified according to the steps similar to those in the above-described verification after effecting new feature options. Specifically, unit 210 stores in buffer 241 authorization code 600 entered by the user, as indicated at step 701 in Fig. 7. At step 702, unit 210 causes the decryption of encrypted option segment 610 of authorization code 600 in buffer 241, thereby recovering the underlying option number (vi). Such decryption is accomplished using a decryption algorithm inverse to the second encryption algorithm. At step 703, processor 201 stores the recovered option number in buffer 243, although in this instance the recovered option number is identical to current option number in buffer 243. At step 704, unit 210 runs the CRC algorithm on the latest code of postage generation program 300, thereby obtaining item (v). At step 705, unit 210 reads the above items (i) through (iv) from memory 200, where item (iv) has the latest software version number of program 300. At step 706, unit 210 independently generates an electronic signature using items (i) through (vi), and the first encryption algorithm in a similar manner to processor 130 generating electronic signature 605 in data center 125. Unit 210 at step 707 compares the generated electronic signature with electronic signature 605 of authorization code 600 in buffer 241. The authorization code is validated if unit 210 finds that the two electronic signatures match.

processor 130 in data center 125 performs initial handshaking with franking system 100 according to a pre-agreed upon communication protocol, thereby identifying at step 815 franking system 100, e.g., by its PSD serial number. Based on the PSD serial number, processor 130 at step 818 locates in database 140 the record pertaining to franking system 100.

At step 821, processor 130 reviews fields 163 and 165 of the located record for the current escrow account balance and configuration information of system 100, respectively. Based on the current configuration of system 100, processor 130 at step 824 causes computer 105 to display a menu thereon containing selections of any new software available for downloading, and currently disabled options for activation. The menu also indicates the current escrow account or credit balance, the prices for downloading any new software having a new version number, and for activating one or more of the disabled options. Assuming that in this example the user wants to activate a previously disabled option, say, option A in the menu, the user may use a mouse device (not shown) attached to computer 105 to select option A.

At step 827, computer 105 communicates the user's selection of option A to processor 130. Upon receiving the option selection, processor 130 at step 830 debits the price of option A from the current escrow account balance, resulting in a new balance in field 163. Accordingly, processor 130 at step 833 changes the value of the bit in the option number (f) in field 165 corresponding to option A, reflecting an activation of option A. At step 836, processor 130 generates authorization code 600 consisting of electronic signature 605 and encrypted option segment 610. As mentioned

generation of postage indicia would be halted as described before.

Based on the disclosure heretofore, it is apparent to a person skilled in the art that where the user chooses to purchase new software online, instead, the steps in process 800 similarly follow, except that in that case, at step 839 the new software, including the new software version number therein, would be downloaded from data center 125 to system 100, along with the transmission of authorization code 600 thereto.

Variations of the design of the authorization code which call for different verification techniques will now be described. In accordance with a first design variation, the authorization code is generated by encrypting items (a) through (f) using a standard encryption algorithm in data center 125. After such an authorization code is provided to system 100, the latter decrypts the received authorization code using a decryption algorithm inverse to the standard encryption algorithm, thereby recovering the underlying items (a) through (f). Items (i) through (v) are then obtain in system 100 in the manner described before, and compares them with the corresponding, recovered items (a) through (e). The authorization code is validated if the two sets of items match.

If the authorization code of the first design variation is not validated because of certain mismatched items, it may be desirable to show on computer 125 such mismatched items for diagnostic purposes. For example, if it is shown that item (d) does not match item (iv), a wrong software version of program 300 may have been installed in system 100. It may be a manufacturing

field 165 of the record pertaining to system 100 in database 140.

Continuing the above example, assuming that the request for activating feature option C is granted, processor 130 in data center 125 changes the value of the bit in option number (f) corresponding to option C from the previous value "0" to the new value "1" to activate the option, as indicated at step 1103 in Fig. 11. Processor 130 at step 1106 generates electronic signature 905 based on items (a) through (f) in the manner described before, where option number (f) incorporates the new bit value "1" corresponding to option C.

Processor 130 then generates encrypted reconfiguration segment 910. Specifically, at step 1109 processor 130 looks up from the aforementioned registered memory map the memory address corresponding to option C at which the new bit value "1" is pre-stored in memory 200. In this instance, the memory address in question is 1A30. At step 1112, processor 130 encrypts the memory address using the aforementioned second encryption algorithm, resulting in segment 910. Authorization code 900 consisting of electronic signature 905 and encrypted reconfiguration segment 910 is fed to system 100 in a reconfiguration mode either by direct communications or a user entry.

After receiving authorization code 900, unit 210 at step 1203 in Fig. 12 decrypts segment 910 of authorization code 900 using the decryption algorithm inverse to the second encryption algorithm, thereby recovering the memory address 1A30. It should be noted that segment 910 starts from the $(m+1)^{th}$ bit of received authorization code 900. Unit 210 at step 1206 retrieves from memory 200 the bit value "1" corresponding to option

programmed to assume that the first two nibbles of the option memory addresses are always "1A". Thus, when option A needs to be changed, only the offset address "2B" or "2C" needs to be communicated using segment 910 for enabling or disabling the option; when option B needs to be changed, only the offset address "2D" or "2E" needs to be communicated using segment 910 for enabling or disabling the option; when option C needs to be changed, only the offset address "2F" or "30" needs to be communicated using segment 910 for enabling or disabling the option; and so on and so forth.

In a second example where authorization code 900 may be used, to save memory space in memory 200, the storage of "1" and "0" values for each option as set forth in the memory map of Fig. 10 may be totally avoided. Since a change in each option involves changing the corresponding bit value in option number buffer 243 to the opposite value, the encrypted reconfiguration segment 910 only needs to communicate the identities of the feature options which need to be changed. After learning the identities of such options based on segment 910, unit 210 locate the bits in buffer 243 corresponding to the identified options and change their current bit values to the opposite values, respectively.

Thus, in this second example, segment 910 is formed by encrypting codes identifying the respective options to be changed. Various designs of the codes are possible as long as each code uniquely identifies a respective option. For example, for the sake of convenience, the code identifying an option may represent the bit position corresponding to the option in buffer 243. Thus, the code for option A may be "01" representing the first bit position of buffer 243

Unit 210 compares the resulting electronic signature with electronic signature 905 of received authorization code 900, as indicated at step 1317 similar to above-described step 1217. If they match, the authorization code is validated. Otherwise, an "Invalid Authorization Code" message would be displayed on computer 105, and generation of postage indicia would be halted as described before.

We have recognized that for loading new software on system 100 for a program upgrade or installation without changing feature options, authorization code 900 may consist of electronic signature 905 only, i.e., encrypted reconfiguration segment having a zero length. In this illustrative embodiment, an array of memory addresses in memory 200 are allocated to pre-store a quantity of possible version numbers of software, e.g., postage franking program 300. As shown in Fig. 14, for example, version number "1" is pre-stored at memory address 1B12; version number "2" is pre-stored at memory address 1B13; version number "3 is pre-stored at memory address 1B14; and so on and so forth. A version number pointer (not shown) in memory 200 is used to indicate the memory location of the current software version number. Assuming that the current software version number is "2", the pointer has a value of "1B13".

The new software to be loaded onto system 100 contains a header which in this instance includes the memory address at which the new software version number is pre-stored. Let's say the new version number is "3" and the header thus contains the memory address "1B14".

In granting the loading of new software onto system 100, processor 130 in data center 125 generates

In addition, to save memory space in memory 200, the storage of possible software version numbers as set forth in the memory map of Fig. 14 may be totally avoided, especially where the software version number always increments by one when new software is loaded onto system 100. In that case, a counter (not shown) in PSD 110 may be used to keep track of the current software version number. Unit 210 may be programmed to be responsive to loading of new software onto system 100 to cause the counter to increment by one, thereby updating the software version number (iv). After loading of the new software, unit 210 independently generates an electronic signature based on items (i) through (vi). The generated electronic signature is compared with electronic signature 905 generated by data center 125 in part based on the new software version number in (d). If they match, the loading of new software onto system 100 is authorized.

Because system 100 is configured as an open system, a user may freely load additional software onto computer 105, and add to system 100 hardware components, e.g., peripherals to computer 105. An advantage of adopting the open system configuration is that application software, other than postage generation program 300 described above, may be installed by the user on his/her own in computer 105 to interact with, say, program 300, to realize a more comprehensive mailing process. Such other application software may include, e.g., a billing program for charging postage back to different accounts, an envelope program for printing an address and a postage indicium on an envelope, an address cleansing program for correcting mailing addresses, etc.

In accordance with another aspect of the invention, a registration identifier is used to (1) identify a franking-related hardware or software component in a franking system configuration, (2) enforce the pre-approval requirement of such a hardware or software component. To achieve object (1), each pre-approved software component, and hardware component including its utility software is assigned a different registration identifier. A duplicate copy of the registration identifier is registered in memory 135 of data center 125. Thus, data center 125 includes in memory 135 a collection of registration identifiers 145 which identify and are associated with different pre-approved components. The registration identifier collection is updated from time to time as additional software and hardware component pass the standardized tests and become approved.

When each pre-approved component interacts with the postage generation program, the registration identifier in the component is compared with the registered registration identifier. If the two identifiers match or correspond, the component is verified to be pre-approved, thereby achieving object (2).

A pre-approved envelope program having a registration identifier for verification of its pre-approval status will now be described. This envelope program may be purchased from a third-party vendor and installed by the user in computer 105. Because of its pre-approval status, the envelope program includes therein a registration identifier which identifies the program. Figs. 16A, 16B and 16C jointly illustrate the envelope program and interactions with postage generation

data stream representative of the texts of the originating and destination mailing addresses, where the originating mailing address data is preceded by the first ensemble of control characters, and the destination mailing address data is preceded by the second ensemble of control characters. The resulting data stream is formatted pursuant to the protocol required by printer 115. For example, if printer 115 is a printer manufactured by Hewlett-Packard Co., the data stream would be in accordance with the Hewlett-Packard printer control language (HP-PCL).

The envelope program proceeds from step 1621 to step 1623 in Fig. 16B where postage generation program 300 described before is invoked. Upon such an invocation, unit 210 in PSD 110 is interrupted, and requests computer 105 to pass thereto a copy of the registration identifier in the envelope program for examination, as indicated at step 1624. If computer 105 fails to produce a copy of the registration identifier, unit 210 causes computer 105 to display thereon an "Unauthorized Component" message, and prevents generation of any postage indicium, as indicated at step 1625.

Otherwise, if computer 105 produces a copy of the registration identifier of the envelope program, unit 210 at step 1626 compares the registration identifier from computer 105 with each of registration identifiers 245 in PSD 110, which are associated with the pre-approved components which have been verified at least once. At step 1627, unit 210 determines whether a corresponding registration identifier is found amongst registration identifiers 245. Assuming that this is not the first time that the envelope program invokes program 300, and the registration identifier of the envelope

acknowledgment that such a registration identifier is valid, and then terminates the communication connection. In response, unit 210 at step 1639 in Fig. 16C adds the returned registration identifier to registration identifiers 245 in PSD 110 for subsequent verification, obviating the need to have processor 130 involved in the subsequent verification of such a registration identifier. Unit 210 then goes on to help generate a postage indicium, as indicated at step 1642.

Otherwise, if processor 130 at step 1631 fails to locate a corresponding registration identifier amongst registration identifiers 145, processor 130 at step 1645 in Fig. 16B returns only a negative acknowledgement that the received registration identifier is invalid, and terminates the communication connection. In response to the negative acknowledgement, unit 210 returns to step 1625.

After step 1642 in Fig. 16C and execution of program 300, a print image of an appropriate postage indicium is prepared. At step 1648 a printer driver program associated with printer 115 is invoked to print the originating and destination addresses, and postage indicium on an envelope fed to printer 115. As the printer driver program interacts with program 300 to receive the print image of the postage indicium resulting from program 300, printer 115 including the printer driver program needs to be pre-approved. As such, upon the invocation of the printer driver program, unit 210 in PSD 110 is interrupted, and requests computer 105 to pass thereto a copy of the registration identifier in the printer driver program for examination, as indicated at step 1651. If computer 105 fails to produce a copy of such a registration identifier, unit 210 denies the

hardware configuration of the computer (i.e., item (b)), the enabled or disabled options (i.e., item (f)), the version of the postage generation program (i.e., item (d)), and other hardware and software components interacting with the postage generation program in the franking system. Such information in database 140 can be used by a postal authority to effectively monitor and control the configurations of individual franking systems in the field.

The foregoing merely illustrates the principles of the invention. It will thus be appreciated that those skilled in the art will be able to devise numerous other arrangements which embody the principles of the invention and are thus within its spirit and scope.

For example, to further deter unauthorized reconfiguration of system 100, the encryption algorithms for generating authorization codes may be changed from time to time. The new algorithms may easily be downloaded from data center 125 during a software upgrade in computer 105, or during a TMS transaction with data center 125. The memory locations in the memory maps of Figs. 10 and 14 may be changed from time to time, as well.

In addition, in the illustrative embodiment, the memory of computer 105 is distinguished from memory 200 in PSD 110. However, the memory spaces in the two memories may be interchangeable in that some or all of the memory contents in memory 200 may be stored in the memory of computer 105, and vice versa. Similarly, some or all of the tasks performed by processing unit 210 in PSD 110 in the illustrative embodiment may be performed by computer 105, and vice versa.

Claims

1. A franking system comprising:

a memory for storing a software component for generating at least one postage indicium;

a device for receiving an authorization code which is derived from at least information concerning the software component; and

a processing unit for verifying at least part of the authorization code to detect any change in the software component before the at least one postage indicium is generated.

2. The system of claim 1 wherein the information represents a version number of the software component.

3. The system of claim 2 further comprising a counter for keeping track of the version number of the software component.

4. The system of claim 2 wherein memory locations are allocated in the memory for storing a plurality of version numbers of the software component, respectively, the version number of the software component being indicated as stored at one of the memory locations.

5. The system of claim 1 wherein the information is obtained from running a predetermined algorithm on code of the software component.

6. The system of claim 5 wherein the information includes error checking information.

14. The system of claim 13 further comprising software components for providing feature options in the system which are selectively enabled, wherein the configuration concerns at least a setting of the feature options.

15. The system of claim 13 wherein the configuration concerns at least a version of the software component.

16. The system of claim 13 further comprising a device for maintaining a postage fund for postage dispensation in the system, wherein the processing unit is within the device.

17. The system of claim 16 wherein the authorization code is also derived from an identity of the device.

18. The system of claim 17 wherein the identity of the device includes a serial number thereof.

19. The system of claim 13 further comprising a computer where the memory is in, wherein the authorization code is also derived from an identity of the computer.

20. The system of claim 19 wherein the identity of the computer includes a serial number thereof.

21. A franking system for generation of postage indicia, the system having a plurality of feature options which may be enabled, the system comprising:

a device for receiving an authorization code which is generated outside the system in response to a request for a selected setting of the feature options different from a current setting thereof, the authorization code

26. The system of claim 25 wherein the data includes offset memory addresses which are associated with the one or more of the feature options, respectively.

27. The system of claim 24 wherein the data identifies the one or more of the feature options.

28. A franking system comprising:

a first memory for storing a first software component for realizing at least one postage indicium, a second software component being stored in the first memory for interacting with the first software component, the second software component including a selected identifier;

a second memory for storing a plurality of identifiers; and

a processing unit for determining whether one of the plurality of identifiers corresponds to the selected identifier in the second software component when the second software component interacts with the first software component, the at least one postage indicium being realized only when one of the plurality of identifiers corresponds to the selected identifier.

29. The system of claim 28 further comprising a device for maintaining a postage fund for postage dispensation in the system, wherein the second memory is within the device.

30. The system of claim 28 wherein the selected identifier identifies the second software component.

36. The system of claim 32 wherein the memory also stores information concerning a current configuration of the franking apparatus.

37. The system of claim 36 wherein the processor causes transmission of a menu to the franking apparatus for the reconfiguration thereof, the menu being generated based on the information.

38. A method for use in a franking system comprising:

storing a software component for generating at least one postage indicium;

receiving an authorization code which is derived from at least information concerning the software component; and

verifying at least part of the authorization code to detect any change in the software component before the at least one postage indicium is generated.

39. The method of claim 38 wherein the information represents a version number of the software component.

40. The method of claim 39 further comprising keeping track of the version number of the software component using a counter in the system.

41. The method of claim 39 further comprising allocating memory locations to store a plurality of version numbers of the software component, respectively, the version number of the software component being indicated as stored at one of the memory locations.

verifying at least part of the authorization code before the at least one postage indicium is generated to detect any change in the configuration of the franking system.

51. The method of claim 50 further comprising providing feature options in the system which are selectively enabled, wherein the configuration concerns at least a setting of the feature options.

52. The method of claim 50 wherein the configuration concerns at least a version of the software component.

53. The method of claim 50 wherein the authorization code is also derived from an identity of a device for maintaining a postage fund for postage dispensation in the system.

54. The method of claim 53 wherein the identity of the device includes a serial number thereof.

55. The method of claim 50 wherein the authorization code is also derived from an identity of a computer.

56. The method of claim 55 wherein the identity of the computer includes a serial number thereof.

57. A method for use in a franking system for generation of postage indicia, the system having a plurality of feature options which may be enabled, the method comprising:

receiving an authorization code which is generated outside the system in response to a request for a

62. The method of claim 61 wherein the data includes offset memory addresses which are associated with the one or more of the feature options, respectively.

63. The method of claim 57 wherein the data identifies the one or more of the feature options.

64. A method for use in a franking system comprising:

storing a first software component for realizing at least one postage indicium;

storing a second software component for interacting with the first software component, the second software component including a selected identifier;

storing a plurality of identifiers;

determining whether one of the plurality of identifiers corresponds to the selected identifier in the second software component when the second software component interacts with the first software component; and

realizing the at least one postage indicium when one of the plurality of identifiers corresponds to the selected identifier.

65. The method of claim 64 wherein the selected key identifies the second software component.

66. The method of claim 64 wherein the second software component includes utility software for interfacing the first software component with at least one hardware component in the system.

reconfiguration thereof, the menu being generated based on the information.

FIG. 4

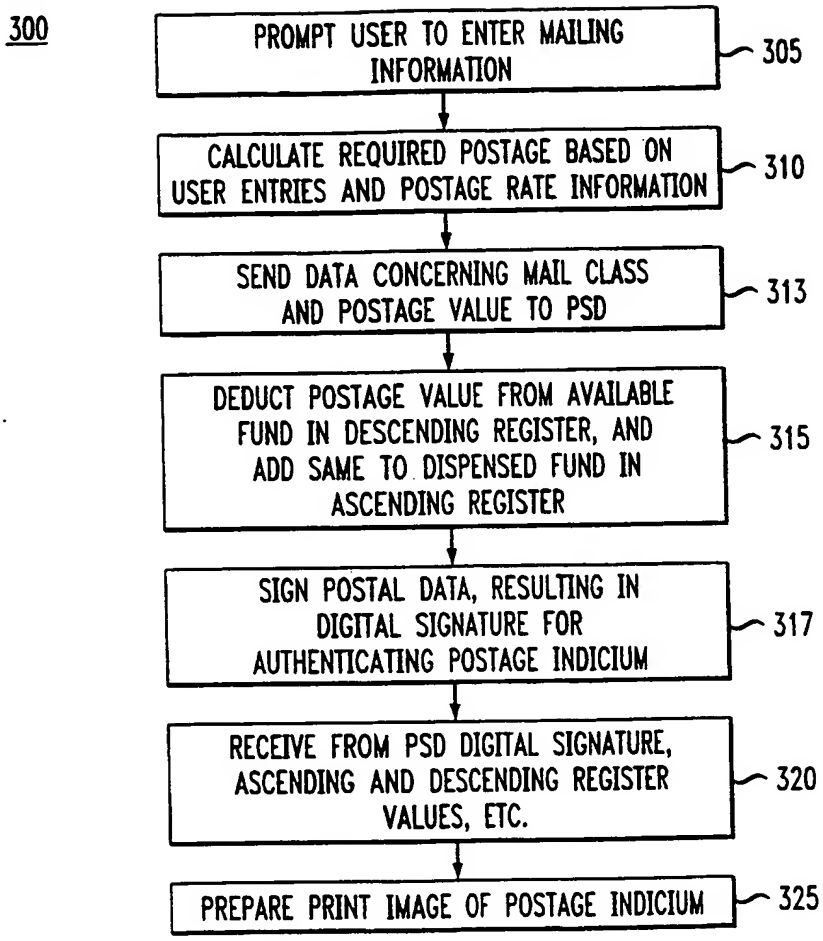

300
PROMPT USER TO ENTER MAILING INFORMATION
305
CALCULATE REQUIRED POSTAGE BASED ON USER ENTRIES AND POSTAGE RATE INFORMATION
310
SEND DATA CONCERNING MAIL CLASS AND POSTAGE VALUE TO PSD
313
DEDUCT POSTAGE VALUE FROM AVAILABLE FUND IN DESCENDING REGISTER, AND ADD SAME TO DISPENSED FUND IN ASCENDING REGISTER
315
SIGN POSTAL DATA, RESULTING IN DIGITAL SIGNATURE FOR AUTHENTICATING POSTAGE INDICIUM
317
RECEIVE FROM PSD DIGITAL SIGNATURE, ASCENDING AND DESCENDING REGISTER VALUES, ETC.
320
PREPARE PRINT IMAGE OF POSTAGE INDICIUM
325

FIG. 5

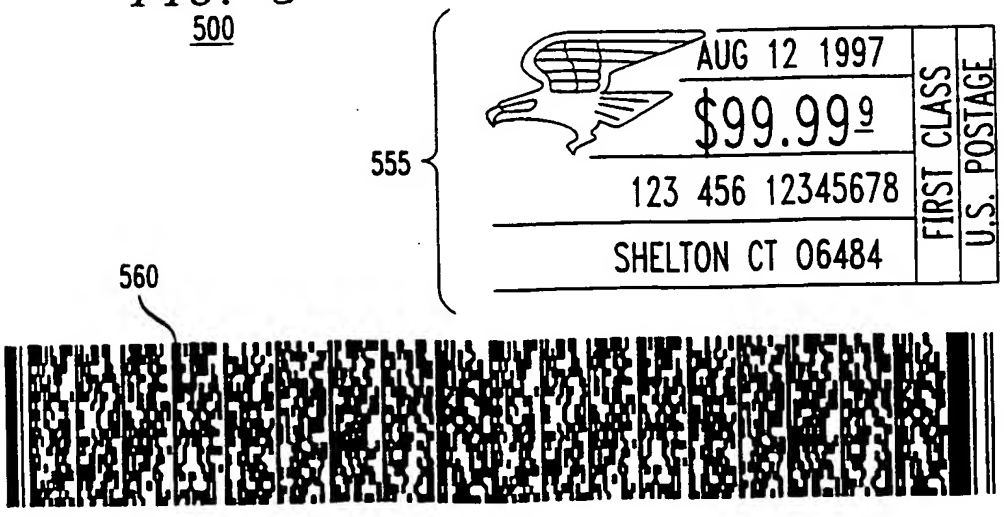

500
555
AUG 12 1997
$99.99
123 456 12345678
SHELTON CT 06484
FIRST CLASS
U.S. POSTAGE
560

FIG. 8A

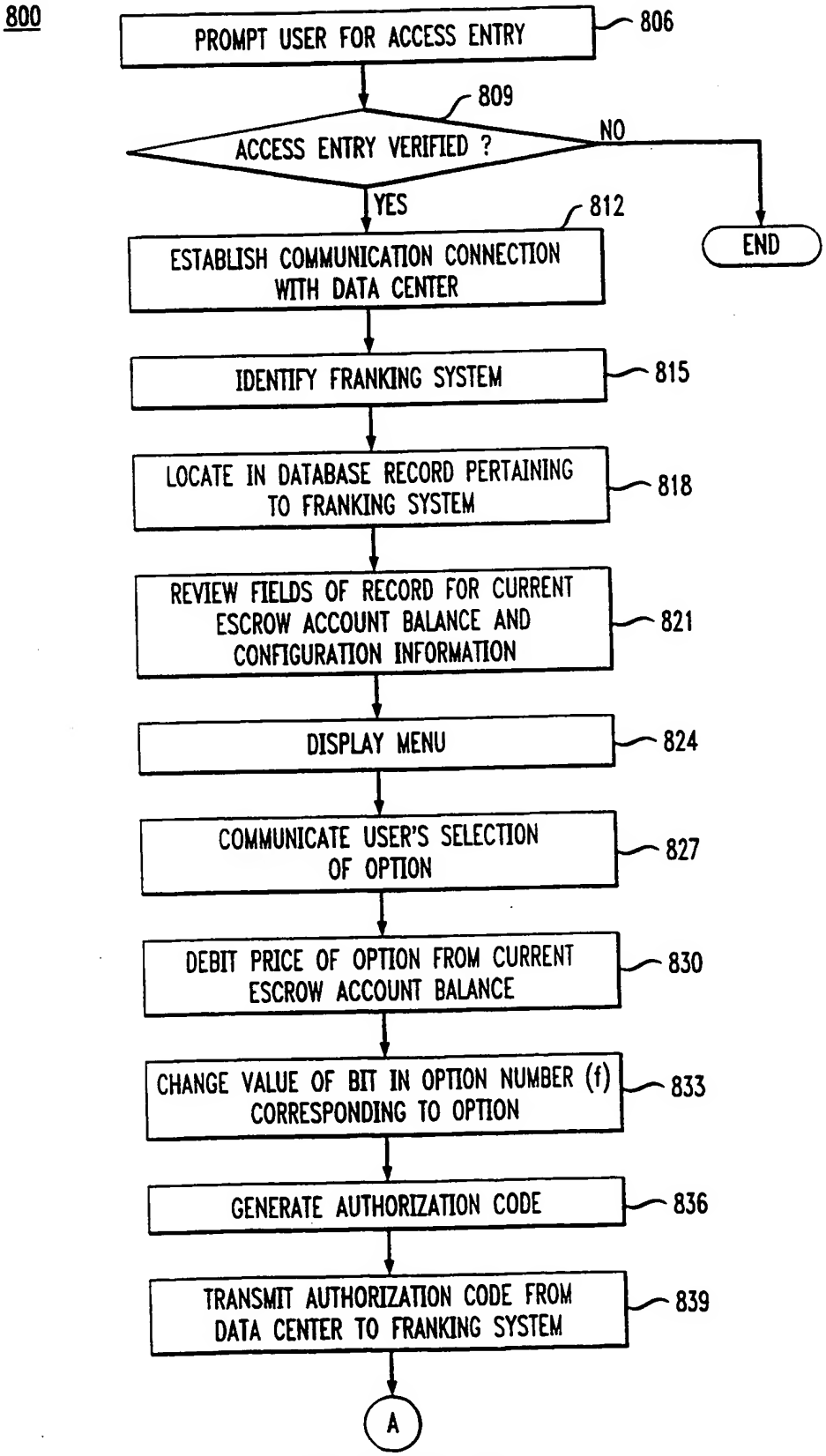

800
PROMPT USER FOR ACCESS ENTRY
806
809
ACCESS ENTRY VERIFIED ?
NO
YES
END
812
ESTABLISH COMMUNICATION CONNECTION WITH DATA CENTER
IDENTIFY FRANKING SYSTEM
815
LOCATE IN DATABASE RECORD PERTAINING TO FRANKING SYSTEM
818
REVIEW FIELDS OF RECORD FOR CURRENT ESCROW ACCOUNT BALANCE AND CONFIGURATION INFORMATION
821
DISPLAY MENU
824
COMMUNICATE USER'S SELECTION OF OPTION
827
DEBIT PRICE OF OPTION FROM CURRENT ESCROW ACCOUNT BALANCE
830
CHANGE VALUE OF BIT IN OPTION NUMBER (f) CORRESPONDING TO OPTION
833
GENERATE AUTHORIZATION CODE
836
TRANSMIT AUTHORIZATION CODE FROM DATA CENTER TO FRANKING SYSTEM
839
A
TO STEP 841 (FIG. 8B)

FIG. 9

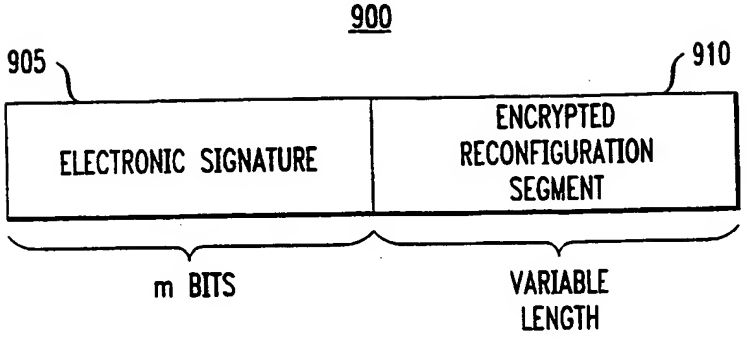


FIG. 10

	MEMORY ADDRESS	MEMORY CONTENT
FEATURE OPTION A	1A2B	0
	1A2C	1
FEATURE OPTION B	1A2D	0
	1A2E	1
FEATURE OPTION C	1A2F	0
	1A30	1

FIG. 11

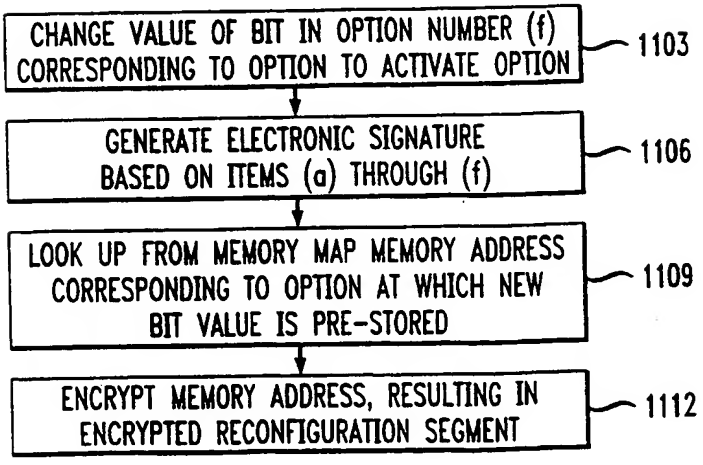


FIG. 14

MEMORY ADDRESS	SOFTWARE VERSION NUMBER
1B12	1
1B13	2
1B14	3
⋮	⋮

FIG. 15

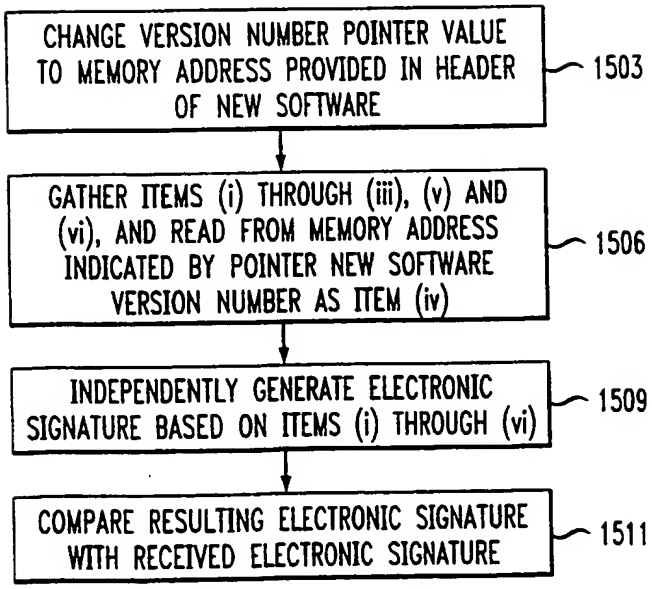
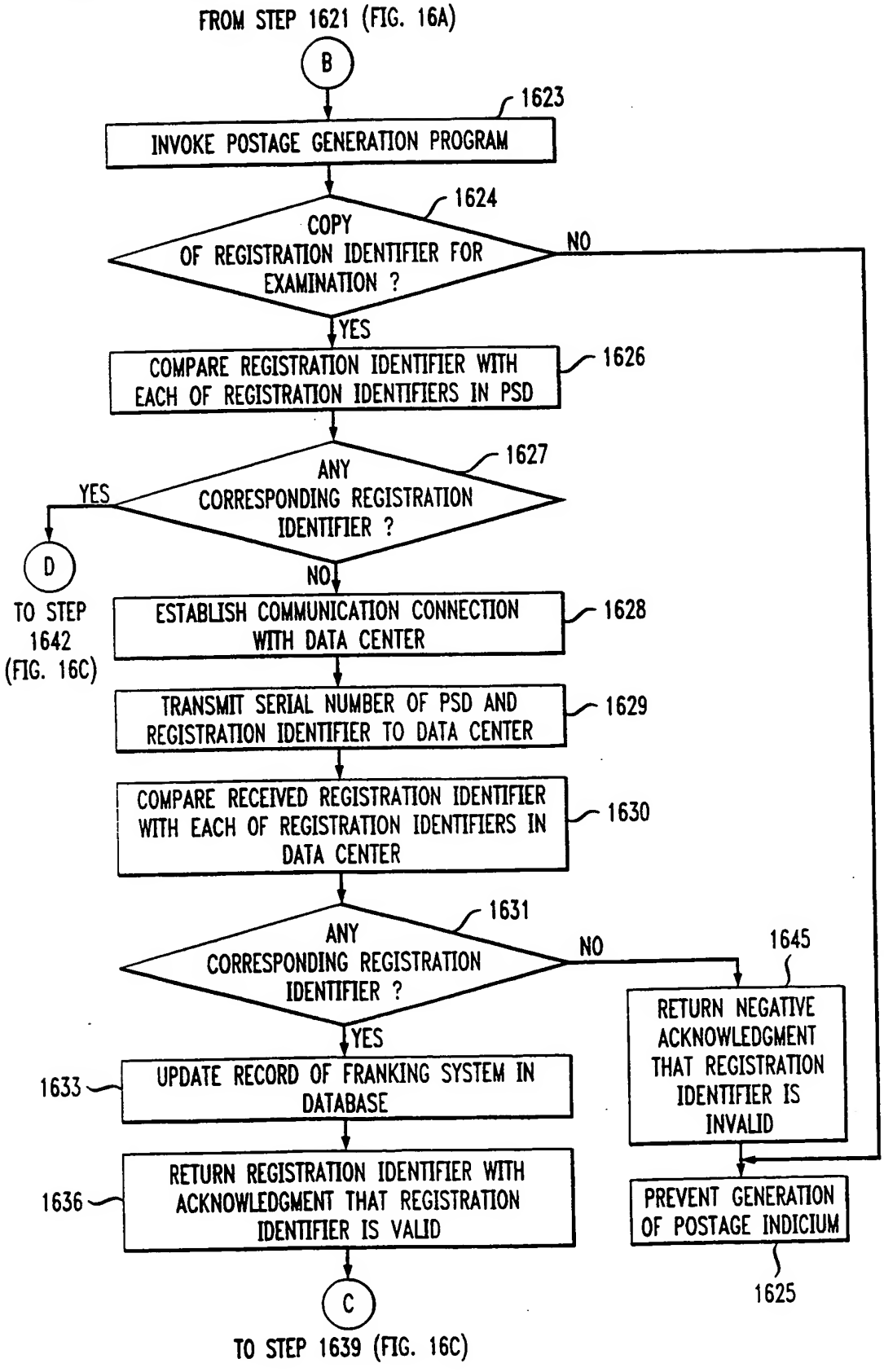


FIG. 16B



INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/13488

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) : G06F 17/00
US CL :705/401

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 705/401

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 4,802,218 A (WRIGHT et al) 31 January 1989, Fig. 8, entire document	1-63
Y,P	US 5,852,813 A (GUENTHER et al) 22 December 1998, entire document	1-63
Y	US 5,680,463 A (WINDEL et al) 21 October 1997, entire document	1-63

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 12 AUGUST 1999	Date of mailing of the international search report 05 OCT 1999
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer E. TODD VOELTZ Telephone No. (703) 308-3900

Form PCT/ISA/210 (second sheet)(July 1992) *

CORRECTED VERSION*

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 17/00

A1

(11) International Publication Number: WO 99/66422

(43) International Publication Date: 23 December 1999 (23.12.99)

(21) International Application Number: PCT/US99/13488

(22) International Filing Date: 15 June 1999 (15.06.99)

(30) Priority Data:
60/089,212 15 June 1998 (15.06.98) US

(63) Related by Continuation (CON) or Continuation-in-Part (CIP) to Earlier Application
US 08/485,269 (CIP)
Filed on 7 June 1995 (07.06.95)

(71) Applicant *(for all designated States except US)*: ASCOM HASLER MAILING SYSTEMS, INC. [US/US]; 19 Forest Parkway, P.O. Box 858, Shelton, CT 06484-0904 (US).

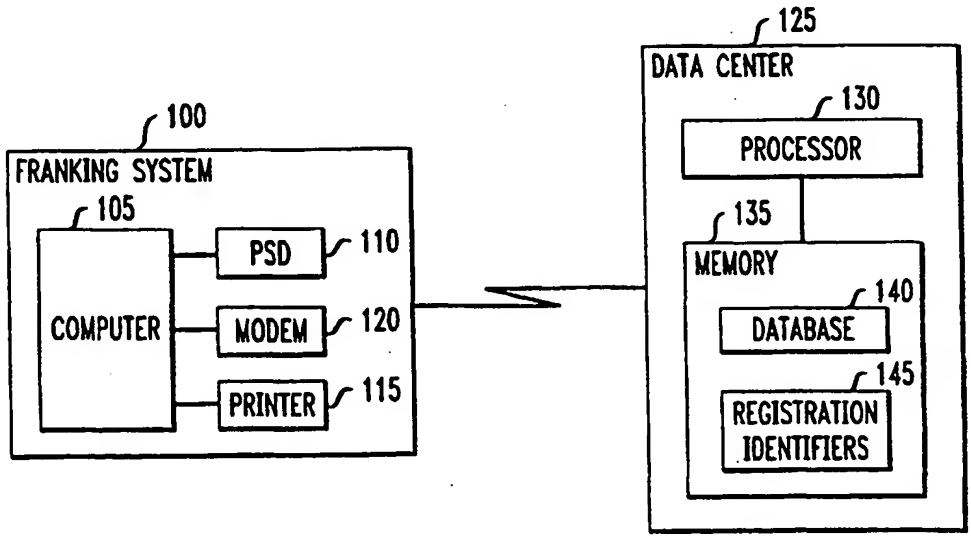
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: SCHWARTZ, Robert, G. [US/US]; 191 Linden Avenue, Branford, CT 06405 (US). BROOKNER, George, M. [US/US]; 11 Surrey Drive, Norwalk, CT 06851 (US). ESKANDARI, Fetneh [IR/US]; 144 Dove Lane, Middletown, CT 06457 (US). CROWE, Allen, A. [US/US]; 76 Klein Drive, Prospect, CT 06712 (US). SIMCIK, Mark, E. [US/US]; 141 Park Avenue, Bloomfield, CT 06002 (US).

(74) Agent: YIP, Alex, L.; Londa & Traub LLP, 37th floor, 20 Exchange Place, New York, NY 10005 (US).

(81) Designated States: CA, JP, US, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: TECHNIQUE FOR SECURING A SYSTEM CONFIGURATION OF A POSTAGE FRANKING SYSTEM



(57) Abstract

In a franking system a postal security device (PSD) tracks a postage fund for dispensing postal indicia and enforce the configuration of the franking system. An authorization code, which is particular to the system, is used to verify the system configuration. An unauthorized change in the system configuration causes invalidation of the code and generation of the postal indicia is denied. Data center (125) records configuration information of each franking system (100). The data center generates a valid authorization code for verification in the franking system based on new configuration information. Components added to the system must be preapproved to prevent fraudulent generation of postage indicia. A registration identifier is assigned to each preapproved component which is necessary for interaction with the franking system.

*(Referred to in PCT Gazette No. 09/2000, Section II)